4-3

УДК 519.22; 004.415.24

В.К. Задирака, Н.В. Кошкина, Л.Л. Никитенко
Институт кибернетики имени В.М. Глушкова НАН Украины, г. Киев, Украина
K_n_v@ukr.net

Статистический анализ систем с цифровыми водяными знаками

В работе рассмотрен статистический подход к построению и оценке качества модели стеганографической системы с цифровыми водяными знаками. Описан метод качественной оценки детектора и декодера ЦВЗ, позволяющий гарантировать определенный уровень надежности. Показан путь построения оптимального детектора и декодера для систем маркировки, базирующихся на методике расширения спектра сигнала. Даны соотношения статистических решающих тестов для детектора при известном вероятностном распределении множества возможных изображений и при приведении гистограммы изображений к фиксированному виду.

Введение

Представление, хранение и распределение информации в цифровом виде давно стали повсеместно используемыми, привычными и удобными манипуляциями над ней. Вместе с тем легкость восстановления и коррекции данных, возможность использования универсальных средств работы над ними и другие преимущества цифрового представления информации могут нивелироваться простотой получения и распространения копий цифровых объектов, полностью идентичных оригиналу. Это влечет за собой необходимость активных исследований проблемы защиты авторских прав на цифровую интеллектуальную собственность.

В связи с недостатком теоретических наработок по проблеме систематизации и оценки качества существующего многообразия методов и алгоритмов защиты авторских прав в статье показан пример моделирования этой проблемы для схем с аддитивными цифровыми водяными знаками (ЦВЗ), базирующихся на методике расширения спектра сигнала [1], [2].

В работе рассматривается статистический подход к построению математической модели систем с ЦВЗ, которая в дальнейшем может служить основой для практической разработки эффективных детекторов и декодеров водяного знака. Статья посвящена разработке модели детекторов и декодеров, требующих на входе не наличия оригинального изображения, а только определенных статистических данных о множестве возможных оригинальных изображений (распределение этого множества) или о виде гистограмм изображений.

Такой подход удобен при оценке качества работы системы с ЦВЗ и для сравнительного анализа различных методов и алгоритмов маркировки изображений. Кроме того он позволяет априори задавать определенный уровень качества путем наложения ограничений на допустимый процент ошибок при обнаружении и декодировании водяного знака.

Общая модель системы маркировки изображений и ее характеристики

Пусть владелец авторского права имеет некоторый секретный ключ K, отображающий его право собственности, и хочет защитить свое цифровое изображение X путем внедрения в него сообщения V, состоящего из элементов некоторого конечного дискретного алфавита и однозначно идентифицирующего владельца. Рассмотрим данную задачу, опираясь на блок-схему общей модели системы маркировки изображений (рис. 1).

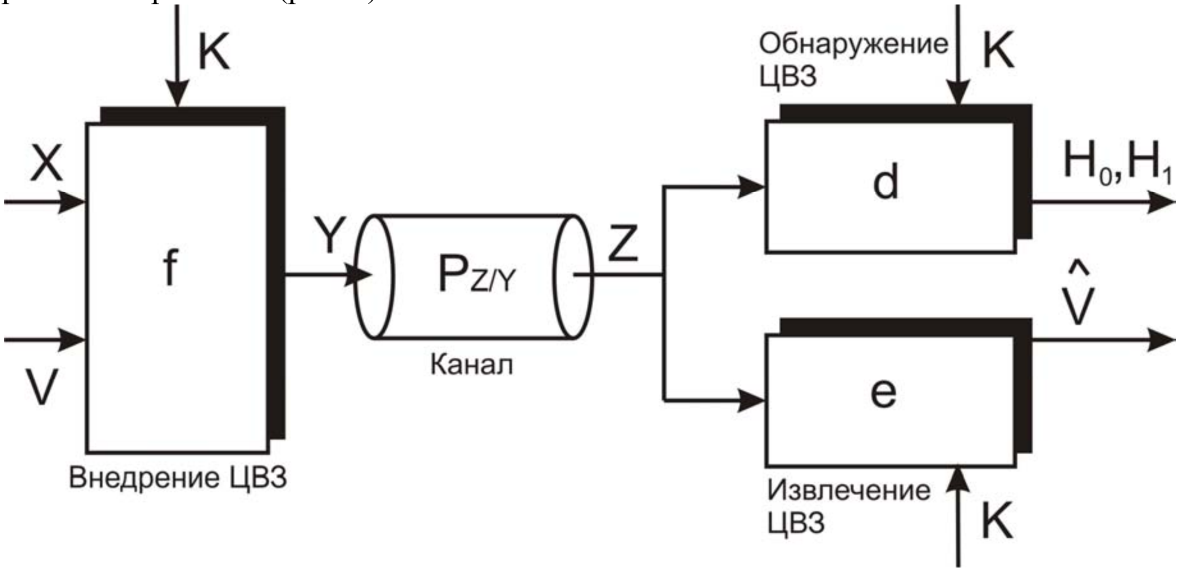


Рисунок 1 – Блок-схема общей модели системы маркировки изображений

Согласно схеме оригинальное изображение X преобразовывается в маркированное изображение Y с помощью функции f, на вход которой также подаются ключ K и сообщение V. Далее изображение Y пересылают получателю по открытому каналу связи, где оно может подвергнуться естественным искажениям, присутствующим в канале, или преднамеренным атакам на ЦВЗ. Причем любые преднамеренные атаки в данном случае выполняются без знания K и X, так как эти элементы публично недоступны. Таким образом, изменения Y можно промоделировать как канал с помехами, вход которого Y и выход Z связаны условным распределением $P_{Z|Y}$.

В процесс проверки авторского права вовлечены две функции: детектор и декодер ЦВЗ. Детектор ЦВЗ d решает, содержит ли изображение Z водяной знак, сгенерированный при помощи ключа K, т.е. на его вход поступают Z и K, а на выходе содержится булево решение. Если детектор определяет наличие водяного знака в изображении, то этим будет доказано авторское право человека, который владеет ключом K. В дальнейшем возможно извлечение скрытого сообщения с помощью декодера ЦВЗ e, на вход которого подаются Z и K, а результатом работы является оценка скрытого сообщения $\hat{V}$. Отметим, что ни у детектора, ни у декодера нет доступа к оригинальному изображению X.

Качественная оценка детектора ЦВЗ выполняется на основе двух критериев – вероятности ложной тревоги P_F и вероятности обнаружения P_D [3]. P_F определяет вероятность получения позитивного результата при тестировании Z на обнаружение ЦВЗ, тогда как фактически это изображение не содержит водяного знака, сгенери-

рованного с ключом K. P_D – вероятность получения позитивного результата тогда, когда изображение действительно содержит ЦВЗ, сгенерированный с ключом K. Пусть H_1 – это гипотеза «изображение содержит ЦВЗ», а H_0 – гипотеза «изображение не содержит ЦВЗ». Тогда

$$P_F \overset{df}{=} \Pr\{d(Z,K) = H_1 \mid H_0\}, \tag{1}$$

$$P_D \overset{df}{=} \Pr\{d(Z,K) = H_1 \mid H_1\}. \tag{2}$$

Качественная оценка декодера ЦВЗ – это вероятность ошибки P_e, определенная как вероятность получения неправильной оценки $\widehat{V}$:

$$P_e \overset{df}{=} \Pr\{\widehat{V} \neq V\}. \tag{3}$$

Соотношения (1) – (3) назовем мерой производительности системы маркировки изображений. Отметим, что при практической реализации детекторов и декодеров особый интерес представляют две следующие условные вероятности ошибок:

$$P_e(X) \overset{df}{=} \Pr\{\widehat{V} \neq V \mid X\}, \tag{4}$$

$$P_e(K) \overset{df}{=} \Pr\{\widehat{V} \neq V \mid K\}, \tag{5}$$

где $P_e(X)$ – вероятность ошибки, обусловленная для данного оригинального изображения X, $P_e(K)$ – вероятность ошибки, обусловленная для определенного ключа K. Первая вероятность показывает, насколько данное изображение подходит для сокрытия в нем сообщения, а вторая – среднюю производительность для конкретного владельца авторского права.

Система маркировки, использующая методику расширения спектра

Многие из существующих методов и алгоритмов создания ЦВЗ так или иначе эксплуатируют методику расширения спектра или, другими словами, широкополосную модуляцию. Методика широкополосной модуляции позаимствована из теории связи [1], [2]. Дело в том, что сокрытие данных можно рассматривать как коммуникационную проблему, в которой оригинальное изображение играет роль шума канала, а атакующие могут попытаться разрушить передачу информации.

Пусть необходимо скрыть N информационных бит в изображении $X = (x_1, x_2 \dots x_L)$, где L – количество элементов в нем. Для этого сначала с помощью генератора псевдослучайных чисел (ПСЧ), инициализируемого с помощью ключа K, образуется псевдослучайная последовательность $S = (s_1, s_2 \dots s_L)$. Далее для того, чтобы гарантировать невидимость водяного знака, S поэлементно перемножается с перцепционной маской δ [4]. Чтобы получить перцепционную маску, используют психовизуальную модель, которая строится на основе учета свойств системы человеческого зрения (СЧЗ). Перечислим некоторые из этих свойств:

– яркостная чувствительность (СЧЗ более чувствительна к шуму на участках с малой яркостью);

– частотная чувствительность (глаз более восприимчив к низкочастотному, чем к высокочастотному шуму);
– эффект маскирования (аддитивный шум гораздо заметнее на гладких участках изображения, нежели на высокочастотных);
– чувствительность к контрасту (глаз наиболее чувствителен к изменениям высококонтрастных участков);
– чувствительность к размеру (большие детали заметнее);
– чувствительность к цвету (некоторые цвета, например, красный заметнее других);
– чувствительность к местоположению (человек обращает больше внимания на центральную часть изображения) и т.д.

Построенная на основе вышеперечисленных свойств маска δ учитывает, как изменение отдельных элементов изображения влияет на его полное перцепционное искажение. То есть с помощью δ добиваются максимальной визуальной незаметности ЦВЗ. Набор индексов $\{1,2\ldots L\}$ разделяют на подмножества $\{\Omega_i\}_{i=1}^{N}$, так что $\forall i \neq j \;\; \Omega_i \cap \Omega_j = \varnothing$. В дальнейшем в каждый Ω_j будет внедрен j-ый бит сообщения. Для обеспечения дополнительной стойкости к атакам такое деление может быть зависящим от ключа. Водяной знак генерируется согласно правилу

$$w_{i,j} = v_j \delta_i s_i, \;\; \forall i \in \Omega_j, \tag{6}$$

где $j \in \{1,2\ldots N\}$, а коэффициент v_j кодирует j-ый бит скрываемого сообщения.

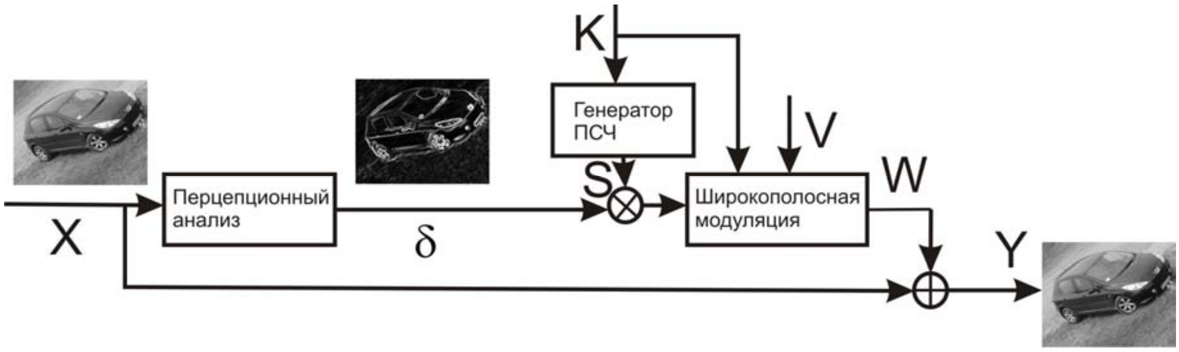


Рисунок 2 – Схема маркировки изображения, использующая методику расширения спектра

В матричном виде

$$W = A(K, X)V, \tag{7}$$

где $V \overset{df}{=} (v_1, v_2 \ldots v_N)^T$ – скрытое сообщение, а $A(K, X)$ – матрица размером $L \times N$, элементы которой удовлетворяют условию:

$$a_{ij} = \begin{cases} \delta_i s_i, & i \in \Omega_j \\ 0, & i \notin \Omega_j \end{cases}. \tag{8}$$

Столбцы матрицы $A = (a_1, a_2 \ldots a_N)$ назовем модуляционными импульсами, так как цифровой водяной знак может быть выражен как их линейная комбинация, что можно сравнить со схемами мультиимпульсной амплитудной модуляции [5], [6].

Итоговое маркированное изображение формируется как сумма оригинального изображения и водяного знака $Y = X + W$ (рис. 2).

Таким образом, в процессе генерирования ЦВЗ вектор скрываемого сообщения, определенный в N-мерном пространстве, случайным образом отображается на пространство большей размерности $(L >> N)$, что в теории связи и называют методикой расширения спектра (Spread Spectrum).

Получение изображения с заданной гистограммой (плотностью распределения)

Источником получения полезной статистики об изображении является гистограмма. Перед тем, как выполнять маркировку изображения согласно схеме, описанной в предыдущем разделе, мы предлагаем привести его гистограмму к заданному, заранее определенному виду. Более того, если известно множество всех возможных оригинальных изображений, мы предлагаем выполнить приведение гистограммы для каждого изображения из этого множества.

Пусть дано некоторое оригинальное необработанное изображение $G = (g_1, g_2 \ldots g_L)$. Яркость пикселей изображения $I(G)$ является дискретной случайной величиной с функцией распределения $P(G) = \{P_i(G)\}$, где $P_i(G)$ – оценка вероятности появления пикселя со значением яркости I_i, $i \in \{0,1\ldots M-1\}$, M – количество уровней яркости. Функцию $P_i(G)$ называют также нормализованной гистограммой цифрового изображения G: $P_i(G) = \dfrac{r_i(G)}{L}$, $\sum_{i=1}^{M} P_i(G) = 1$, где $r_i(G)$ – количество пикселей с яркостью I_i, L – общее количество пикселей в изображении.

Изображение G необходимо преобразовать таким образом, чтобы его яркость имела априори заданное распределение $P(X) = \{P_j(X)\}$, $j \in \{0,1\ldots M-1\}$. Будем считать, что уровни яркости упорядочены по возрастанию.

Алгоритм отображения $P(G)$ в $P(X)$ имеет вид:

Шаг 1.

1) если $P_0(G) = P_0(X)$, то ничего не делаем;
2) если $P_0(G) > P_0(X)$, то количество пикселей в исходном изображении $r_0(G)$ нужно уменьшить до величины $r_0(X)$ путем увеличения яркости $|r_0(X) - r_0(G)|$ пикселей;
3) если $P_0(G) < P_0(X)$, то количество пикселей в исходном изображении $r_0(G)$ нужно увеличить до величины $r_0(X)$ путем уменьшения яркости более ярких $|r_0(X) - r_0(G)|$ пикселей в G до I_0;
4) пересчитываем вероятности $P_i(G)$ после сделанных преобразований.

Шаг 2. Имеем $P_0(G) + P_1(G) = P_0(X) + P_1(G) = P_G(I_1)$,

$$P_0(X) + P_1(X) = P_X(I_1).$$

1) если $P_1(G) = P_1(X)$, то ничего не делаем;
2) если $P_1(G) > P_1(X)$, то количество пикселей в текущем изображении с яркостью I_1 нужно уменьшить путем увеличения яркости $|r_1(X) - r_1(G)|$ пикселей;

3) если $P_1(G) < P_1(X)$, то в изображении G выбирается $|r_1(X) - r_1(G)|$ пикселей с яркостью, большей нежели I_1 и их яркость уменьшается до I_1;

4) пересчитываем вероятности $P_i(G)$.

Третий и все последующие шаги выполняются аналогично второму шагу.

Статистическая задача о выборе из двух гипотез

Рассмотрим функционирование детектора ЦВЗ как решение статистической задачи проверки основной гипотезы H_0 – «изображение не содержит ЦВЗ», при условии, что для нее имеется всего одна альтернатива, гипотеза H_1 – «изображение содержит ЦВЗ». Цель раздела состоит в описании критерия выбора из двух гипотез, что в дальнейшем позволит конструировать оптимальные тесты на обнаружение водяного знака.

Всякое правило принятия решения характеризуется вероятностью принять ту или иную гипотезу в зависимости от наблюдаемого значения случайной величины Z. Пусть $\pi(Z)$ есть «критическая» вероятность – вероятность отвергнуть основную гипотезу, если наблюдаемое изображение есть Z, т.е.

$$\pi(Z) = P(H_1 \mid Z) \tag{9}$$

(вероятность принять гипотезу H_1 о наличии ЦВЗ в изображении при условии, что наблюдалось Z). Качество правила определяется вероятностями принятия и отвержения каждой из гипотез в зависимости от того, какая из гипотез верна. Его характеризуют вероятностями ошибок.

Ошибка первого рода – отвергнуть истинную основную гипотезу H_0, она обычно обозначается α

$$\alpha = P(H_1 \mid H_0). \tag{10}$$

Ошибка второго рода – принять основную гипотезу, если верна альтернатива, ее вероятность обозначается β:

$$\beta = P(H_0 \mid H_1). \tag{11}$$

α – уровень значимости критерия, $1-\beta$ – его мощность [7]. Согласно введенным в первом разделе обозначениям $\alpha = P_F$ (уровень значимости соответствует вероятности ложной тревоги для детектора ЦВЗ), $1-\beta = P_D$ (мощность – это вероятность обнаружения ЦВЗ детектором). Уровень значимости выбирается заранее. В нашем случае при выборе нужно исходить из коммерческой целесообразности допустимости ложной тревоги для системы с ЦВЗ, например, уровень значимости 1 %, при этом $\alpha = 0{,}01$. Мощность критерия максимизируют, т.е. вероятность ошибки второго рода стараются сделать минимальной. Если выбрана критическая вероятность, то

$$\alpha = \int \pi(Z)F_0(dZ), \ \beta = \int (1-\pi(Z))F_1(dZ), \tag{12}$$

где $F_i(Z)$ – распределение величины при гипотезе $H_i (i = 0,1)$.

Наиболее «мощный» критерий с заданным уровнем значимости – критерий Неймана-Пирсона. Он определен для случая, когда мера F_1 абсолютно непрерывна

относительно меры F_0: для всех борелевских множеств $C \in R^m$

$$F_1(C) = \int_C f(Z) F_0(dZ). \quad (13)$$

Рассмотрим два важных случая, когда равенство (13) выполнено.

1) Пусть F_1 и F_2 имеют плотности относительно лебеговой меры в R^m, равные $f_1(Z)$ и $f_2(Z)$ соответственно, причем $f_0 > 0$. Тогда равенство (13) выполняется, если

$$f(Z) = \frac{f_1(Z)}{f_0(Z)}. \quad (14)$$

2) Пусть обе меры $F_i(dZ)$ дискретны, т.е. можно указать такую последовательность $Z_i \in R^m$, что $\sum F_0(\{Z_i\}) = \sum F_1(\{Z_i\}) = 1$ и $F_0(\{Z_i\}) > 0$ для всех Z_i. Тогда

$$f(Z_i) = \frac{F_1(\{Z_i\})}{F_0(\{Z_i\})} \quad (15)$$

(значения $f(Z)$ при $Z \neq Z_i$ роли не играют).

Пусть J_t – такое множество, что $f(Z) \geq t$ при $Z \in J_t$, $f(Z) \leq t$ при $Z \in R^m - J_t$. При $F_0(J_t) = \alpha$ критерий является наиболее «мощным» при уровне значимости α для непрерывного случая. Кроме того всегда можно разделить R^m на два множества $D_{t\alpha}$ и $R^m - D_{t\alpha}$ такие, что $f(Z) \geq t_\alpha$ на $D_{t\alpha}$ и $f(Z) \leq t_\alpha$, на $R^m - D_{t\alpha}$ и $F_0(D_{t\alpha}) = \alpha$.

Для дискретного случая R^m делится на три множества $D_{t\alpha}$, где $f(Z) > t_\alpha$, Γ_α, где $f(Z) = \alpha$, и $R^m - D_{t\alpha} \cup \Gamma_\alpha$. Если $\pi(Z)$ для критерия выбирается как

$$\pi(Z) = \begin{cases} 1, Z \in D_{t\alpha} \\ p, Z \in \Gamma_\alpha \\ 0, Z \in R^m - D_{t\alpha} \cup \Gamma_\alpha \end{cases},$$

и

$$\alpha = pF_0(\Gamma_\alpha) + F_0(D_{t\alpha}),$$

то критерий также является наиболее «мощным».

Построение оптимальных структур детектора и декодера ЦВЗ как решение статистической задачи

Пусть имеется изображение Z и ключ K, а также предполагается, что маркированное изображение не переносило ни неумышленных искажений, ни атак, т.е. $Z = Y$. Цель теста на обнаружение ЦВЗ состоит в том, чтобы решить, содержит ли изображение Z водяной знак, сгенерированный владельцем авторского права, который обладает ключом K. Этот тест можно сформулировать как бинарный тест двух гипотез:

$$H_1: \ Z = X_1 + A(K, X_1)V,$$
$$H_0: \ Z = X_0, \quad (16)$$

где X_1 и X_0 – какие-то изображения. Так как декодировать скрытое сообщение в данном случае не обязательно, элемент V рассматривается как случайный вектор с функцией распределения, равной вероятности распределения сообщения.

Чтобы убрать зависимость A от неизвестного детектору оригинального изображения, $A(K,X)$ разумно аппроксимировать заменой на $A(K,Z)$, так как ЦВЗ привносит в изображение небольшие искажения, которые ожидаемо повлекут за собой незначительные изменения в перцепционной маске δ. Тогда тест (16) можно аппроксимировать следующим бинарным тестом:

$$H_1: \ Z = X_1 + A(K,Z)V,$$
$$H_0: \ Z = X_0. \qquad (17)$$

Пусть $S \in \{H_1, H_0\}$ – решение, полученное при тесте на обнаружение ЦВЗ (функция d на рис. 1). Чтобы гарантировать надежность системы маркировки изображений, вероятность ложной тревоги, определяемая как $P_F = \Pr\{S = H_1 \mid H_0\}$, должна быть ниже некоторого максимального значения (порога). При разработке детектора преследуется цель максимизировать вероятность $P_D = \Pr\{S = H_1 \mid H_1\}$, которая соответствует максимально допустимому P_F.

В тесте на декодирование ЦВЗ предполагается, что Z действительно содержит водяной знак, принадлежащий обладателю авторского права, владеющему секретным ключом. Цель декодера состоит в том, чтобы получить оценку $\hat{V}$ вектора сообщения V таким образом, чтобы минимизировать вероятность ошибки. Для декодера, как и для детектора, матрицу $A(K,X)$ можно аппроксимировать матрицей $A(K,Z)$.

Принимая ключ K фиксированным, можно сказать, что в статистических решающих тестах есть два случайных вектора – X и V. Если известно распределение $f_X(X)$, оптимальные решающие тесты образуются согласно правилу Неймана-Пирсона, рассмотренному в предыдущем разделе. Например, в тесте на обнаружение ЦВЗ оптимальный детектор, который максимизирует P_D для любого значения P_F, задается тестом:

$$\ln \frac{f_Z(Z \mid H_1, K)}{f_Z(Z \mid H_0)} = \ln \sum_V \frac{p(V) f_X(Z - A(K,Z)V)}{f_X(Z)} \underset{H_0}{\overset{H_1}{\gtrless}} \eta, \qquad (18)$$

где η – порог, величина которого зависит от α и распределения $F_0(Z)$ согласно (12). Если принять сообщения равновероятными, то $\forall V \ p(V) = \frac{1}{M}$, где M – количество элементов алфавита, из которого они формируются.

Оптимальный декодер ЦВЗ, который минимизирует вероятность ошибки, обусловленной для ключа K, задается структурой максимальной вероятности:

$$\hat{V} = \arg\max_V \ln f_Z(Z \mid V) = \arg\max_V \ln f_X(Z - AV), \qquad (19)$$

где приставка $\arg$ означает, что ищется не максимальное значение, а номер максимального аргумента функции $\max$.

Выражения (18) и (19) задают функции детектора и декодера, представленных на рис. 1, $d(Z,K)$ и $e(Z,K)$ соответственно.

Если распределение $f_X(X)$ не известно, но известно, что для множества всех возможных оригинальных изображений их гистограммы имеют одинаковый вид – $P(X) = \{P_j(X)\}, j \notin \{0,1 \ldots M-1\}$, то критерий Неймана-Пирсона следует использовать для каждого уровня яркости. Если хотя бы для одного уровня яркости принимается решение в пользу гипотезы H_1, то детектор принимает решение о наличии ЦВЗ. Оптимальные решающие тесты для каждого уровня яркости j получаются из условия

$$\frac{P_j(Z \mid H_1, K)}{P_j(Z \mid H_0)} = \frac{P_j(Z)}{P_j(X)} \begin{array}{c} > \\ < \end{array} \lambda , \qquad (20)$$

где λ – порог, $P_j(X)$ и $P_j(Z)$ – вероятности появления j-ого уровня яркости в оригинальном и наблюдаемом изображениях.

Влияние искажений и атак

В процессе распространения маркированное изображение может быть случайно или специально искажено, например, аддитивным шумом, фильтрацией или геометрическими преобразованиями. В целом множество возможных искажений ограничивается искажениями, которые не приводят к чрезмерной деградации изображения, делающей его непригодным к использованию. Искажения и атаки ухудшают производительность решающих тестов. Так как все возможные деформации изображения смоделировать трудно, детектор ЦВЗ следует разрабатывать так, чтобы максимизировать P_D для самого плохого случая, связанного с атакой самого плохого случая. Аналогично декодер следует разрабатывать так, чтобы минимизировать вероятность ошибки P_e для самого плохого случая.

Самая плохая атака для рассмотренной системы маркировки – атака при помощи геометрических преобразований, таких как сдвиг, масштабирование, вращение, обрезка изображения и пр. Чувствительность детектора ЦВЗ к этому виду манипуляций проистекает из «белой» природы псевдослучайной последовательности $S = (s_1, s_2 \ldots s_L)$, что приводит к десинхронизации модуляционных импульсов, фактически представленных в изображении и сгенерированных во время решающего теста. Перспективным подходом для достижения надежности против геометрических искажений является компенсация геометрических преобразований перед извлечением водяного знака либо же внедрение ЦВЗ в инвариантную к геометрическим преобразованиям область [8], [9].

Заключение

В дальнейшей работе планируется продолжить статистический анализ систем маркировки изображений. В частности, для систем, использующих методику расширения спектра, рассмотреть случай построения оптимального декодера при неизвестном распределении оригинальных изображений, но с априори известной единой гистограммой. А также случай, когда гистограмма оригинального изображения не

известна, но известна другая статистическая информация, такая как, например, дисперсия и матрица ковариации [10]. Кроме того планируется рассмотреть применение кодов коррекции ошибок в процессе генерации ЦВЗ, что позволит повысить надежность системы маркировки.

Литература

1. Glisic S., Vucetic B. Spread Spectrum CDMA for Wireless Communications. – Norwood, MA: Artech House, 1997.
2. Viterbi A. CDMA. Principles of Spread Spectrum Communication.Reading. – MA: Addison-Wesley, 1995.
3. Nikolaidis N., Pitas I. Robust image watermarking in the spatial domain // Signal Processing. – May 1998. – V. 66. – P. 385-404.
4. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 261 с.
5. Performance analysis of a 2D-multipulse amplitude modulation scheme for data hiding and watermarking of still images / J.R. Hernandez, F. Perez-Gonzalez, J.M. Rodrıguez, G. Nieto // IEEE J. Select, Areas Commun. – May 1998. – V. 16. – P. 510-524.
6. Sklar B. Digital Communications. Fundamentals and Applications. – Englewood Cliffs, NJ: Prentice-Hall, 1988.
7. Гихман И.И., Скороход А.В., Ядренко М.И. Теория вероятностей и математическая статистика. – К.: Вища школа, 1979. – 408 с.
8. Кошкина Н.В. Методы синхронизации цифровых водяных знаков // Кибернетика и системный анализ. – 2008. – № 1. – С. 180-188.
9. Задирака В.К., Никитенко Л.Л. К вопросу о стойкости стегосистем к обнаружению факта передачи скрываемых сообщений для двух частных случаев // Проблемы управления и информатики. – 2008. – № 3. – С. 152-156.
10. Hernandez J.R., Perez-Gonzalez F. Statistical Analysis of Watermarking Schemes for Copyright Protection of Images // Proc. of the IEEE. – July 1999. – V. 87, № 7. – P. 1142-1166.

В.К. Задірака, Н.В. Кошкіна, Л.Л. Нікітенко

Статистичний аналіз систем з цифровими водяними знаками

У роботі розглянуто статистичний підхід до побудови та оцінки якості моделі стеганографічної системи з цифровими водяними знаками. Описано метод якісної оцінки детектора та декодера ЦВЗ, який дозволяє гарантувати певний рівень надійності. Показано шлях побудови оптимальних детектора та декодера для систем маркування, які базуються на методиці розширення спектра сигналу. Подані співвідношення статистичних вирішуючих тестів для детектора при відомому імовірнісному розподілі множини можливих зображень та при наведенні гістограми зображень до фіксованого виду.

V.K. Zadiraka, N.V. Koshkina, L.L. Nikitenko

The Statistical Analysis of the Watermark Systems

The paper is devoted with approach to the modeling and the quality rate of the steganography system model with the digital watermarks. The quality rate method of the detector and decoder of the digital watermark is defined that is permissive specified guaranteed robustness level. The modeling path of the optimal detector and decoder for the flagging systems is realized that were founded on the signal spread spectrum method. The statistical deciding test relations for the detector are presented when probability distribution of the possible image set was known and when the image histograms ware fixed fashion.

Статья поступила в редакцию 10.07.2008.